GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

Alison Ramsley
December 22, 2003
GIAC Security Leadership Certificate (GSLC)
Practical Assignment
Version 1.0 (April 8, 2002)

Developing a “Security Aware” Culture in an Employee owned Company

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

1. ABSTRACT 1

2. INTRODUCTION 1

3. DEVELOPING SECURITY AWARENESS 2

A. IDENTIFY A SECURITY TEAM RESPONSIBLE FOR INFORMATION SECURITY 3
B. SENIOR MANAGEMENT BUY-IN 3
C. UNDERSTAND THE COMPANY'S RISK 4
D. SECURITY AWARENESS PRESENTATION 5
E. POLICY CREATION & IMPLEMENTATION 6

4. CONCLUSION/SUMMARY 6

REFERENCES 8

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Abstract

When talking about information security, it is often said that your own people are your weakest link. This has been true for many years and continues to be ranked by many as the biggest security threat to most organizations. As famed hacker Kevin Mitnick quoted:

"People are the weakest link. You can have the best technology, firewalls, intrusion-detection systems, biometric devices - and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything."
- Kevin Mitnick[1]

The complexity of this situation is increased many folds in an employee owned organization because many users actually *own* the computer system and therefore feel like they have the right to use it any way they please.

If our owners or employees are our biggest threat then we must educate them and make them aware of the do's and don'ts around information security. The assumption is that companies who strive to develop a security aware culture so that their users act responsibly when it comes to information security, these companies will be more successful in protecting their assets.

This paper will focus on the various steps an employee owned company can take to develop a security aware culture in its organization.

2. Introduction

A good information security strategy is made up of many elements. They include risk identification, external auditing, physical security, incident handling, security policy, intrusion detection, patch management, virus protection and so on. One element that is often overlooked and can be one of the most critical elements to a good security strategy is user awareness.

The goal in developing a security aware culture is to create an environment where users would be less likely to execute viruses, they would understand what social engineering is, they would be less likely to reveal their passwords, they would be more cooperative in protecting the company's assets and they would be aware of what the risks are to the organization.

Having users who understand and are made aware of the concepts behind information security will prove to be an invaluable element in a company's goal to implement a sound security strategy.

[1] CNN.com. Hacker Kevin Mitnick speaks out.
http://www.cnn.com/2000/TECH/computing/09/29/open.mitnick.idg

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Employee owned companies can add another dimension of complexity when implementing a sound information security strategy. Mandating rules and policy from the top down is often not a realistic approach in an employee owned organization. However because it is employee owned, the users will want to protect their assets and will assume that their IT department is protecting them. They want the freedom to do whatever they like with the companies computer systems because they are after all, the owners of the company, yet they assume/expect they are completely protected.

This type of attitude can be a real challenge for an IT department. One strategy to overcome some of these challenges is to educate the owners (employees) of the company and make them aware that the topic of information security is a balancing act between keeping the companies assets secure, allowing access to the resources and doing this all in a cost effective manner. Once people begin to understand that information security is somewhat like "pushing the ocean back with a fork"[2] and it's not as easy as just implementing a password policy, then they will become more aware and help the process.

3. Developing Security awareness

As is the case with most information security concepts, there are many methods to developing security awareness in a company. Although the information security concepts that you want to educate your employees about are fairly standard, the method in which you choose to deliver the concepts will vary. It is important to understand and use what is realistic and what will be successful in your organization. The concept of creating a security aware culture and developing security awareness in your company is about changing or forming habits so you must understand and use a method that will work in the culture that is already established in your organization. Large employee owned companies (many owners) are typically not dictated to from the top down and have a flat management structure. Some of the more traditional methods of implementing security awareness may not be realistic or successful in such an environment.

Outlined below are 5 steps that an organization can look at to begin to develop a successful security aware culture:

The steps identified are as follows:

A. Identify an Information Security Team across the organization
B. Get Senior Management buy-in
C. Understand the companies risk
D. Develop a Security Awareness Presentation
E. Create & Implement Security Policies

[2] Herbeck, Jim; SANS Security Leadership Course Instructor, July, 2003

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The steps do not have to be followed in the order described and it's common that the steps will overlap with each other. It may be necessary to start working on one of the steps and jump to another to assist in completing the previous. The important thing to note is that by addressing all of the steps outlined, you can start to develop an organization that is aware of information security.

A. Identify a Security Team responsible for Information Security

One of the first actions to take is to identify a security team with a strong leader, who will be responsible for the area of information security. Identifying a security team demonstrates to the users that the company is serious about the subject. It assists in getting the topic of information security on the minds of the employees and may even get them to start asking questions like "what is information security all about" and "why do we need an entire team to address this issue?".

A security team will help to put structure around this very broad topic and provide a mechanism for implementing a good security plan. If information security is simply left to the IT folks to handle as part of their mandate, they will invariably all have different perspectives on information security. They will argue about what are the most important aspects of information security which can often lead to fractured information security systems throughout the company including that of security awareness for employees. A fractured information security system can leave the company exposed to vulnerabilities and therefore increase the risk which is contrary to the desired goal.

The security team should include people from across all regions of the company. If your company spans different countries or continents, members of the team should include people from these regions. The mandate of the information security team could include determining the security priorities to be addressed, working with the other IT folks in the company to monitor security elements, creating, delivering and monitoring security awareness concepts throughout the company etc. With the team concentrating on all of the aspects of information security including monitoring the delivery of the security awareness training, the culture of the company will begin to change towards a more aware culture.

B. Senior Management buy-in

The security team or certain members of the team need to also be responsible for meeting with senior management to define the company's risk. In order to create a security aware culture in an organization, senior management must support the efforts. Information security is no longer an IT issue, rather it's a business issue that must be addressed in a formal manner and taken seriously. Cultural changes will not happen easily and may not happen at all if the senior members of the organization don't understand the need for them. In an

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

employee owned company, senior management buy-in can be even more critical because they are the majority owners in the company.

Implementing security practices in a company can often be viewed as negative because they usually require a change in user habits. If the user doesn't understand the significance of these security practices such as why the company is spending money on information security, why the company won't support remote access to the network, why the company mandates the users to change their password on a regular basis, then the process of implementing a sound security strategy will be even more of an arduous task.

Gaining senior management buy-in regarding the importance of information security can be quite challenging because it is difficult to describe its worth when they don't understand the concepts. As part of the senior management buy-in it may make sense to go through your risk identification steps to further explain the importance of it. Dealing with senior management in terms they can understand will prove to make the task much easier.

One strategy that is often successful in obtaining senior management buy-in is to get a "champion" from the senior management team who understands enough about the importance of information security and who also has the trust of the senior management team. Educating this person who can then in turn educate the rest of the senior management team can be quite successful. Depending on the structure of the company, senior management will often listen to and trust one of their own much more quickly and easily then they will trust or understand an IT security team member.

Another strategy you can use if you're having difficulty gaining senior management buy-in is to enlist in an outside consulting firm that specializes in Information security. Senior management in some companies may be more inclined to listening to outside expertise rather then internal resources.

C. Understand the Company's Risk

Once a team has been established, and senior management has bought in to the concept that the company must pay attention to information security, identifying what the risks are to the company and what level of exposure is acceptable is the next step. There are risks everywhere; some of these risks can be irrelevant to your company while others can shut down your business. A company needs to understand what their risks are and then know what to do if those risks become real. The risk identification process can be an overwhelming task and because of this, companies can easily get stuck on this step. One important concept is that the risk is defined through a collaborative effort between the security team and senior management. Senior management's contribution will be to identify what the business risks are to the company, while the security team will identify

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

what the technical information security risks are. Some companies make the mistake of not using the collaborative approach rather they expect the IT departments to identify the company's risk or senior management in isolation to define the risk. Both of these scenarios can result in a poorly defined risk assessment and can lead to excess spending and/or to a false sense of security.

Choosing a formula or matrix that everyone is comfortable with to describe your risk is a good way to put some structure around this daunting task. This approach allows decisions to be made based on facts rather then assumptions and emotions. An example of a formula is: risk = vulnerability x threat x asset value where vulnerability is defined as a weakness in a system that could be exploited, a threat is any event that can cause an undesirable outcome, and asset value can be tangible or intangible and is composed from various elements that are related to the asset[3]. By including asset value in the equation, we're indicating that a higher asset value will indicate a higher risk factor.

After you've completed the risk identification process, your security team can prioritize their tasks and proceed with informing your users about information security and how it relates to the business.

D. Security Awareness Presentation

The first three steps described above will provide a great foundation for creating a security aware culture in your company. The next step will be to create an effective security awareness presentation that will be presented to all of the employees. It's important that a consistent presentation be developed and presented so that the proper information security messages are communicated to all employees. By having members of all regions on the security team, you will get important concepts for each region in to the presentation so that it applies to everyone. Remember to ensure the presentation makes sense in all languages if that's something your company must address. Relaying the proper security message is obviously important so you don't want anything confused when the presentation is translated in to multiple languages.

Once the presentation is complete, the challenge may be to deliver it to all of the users especially if your company spans the globe. Listed are a few strategies that may help the process; use any of the internal training mechanisms a company may have for other courses; hold "brown bag" type sessions; attend group meetings to deliver the presentations; and/or use web cast type technology to target a large audience in different locations.

Understand again, what will be effective in your company and deliver it that way. Ensure you monitor attendance and are confident that everyone in the company has been exposed to the presentation.

[3] Cole, Fossen, Northcutt, Pomeranz; SANS Security Essentials Version 2.1 Volume One; p. 832-833

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

There are new risks, vulnerabilities, tricks every day that leave a company exposed to danger so regular, updated messages regarding information security is another important point in creating a security aware culture. A company must stay on top of this subject and employees need to constantly be informed and reminded about their role in this area. Creating a security aware culture is an on-going task that needs consistent attention and communication.

E. Policy Creation & Implementation

Security policy creation and implementation helps to reinforce the security aware culture. Policy tends to provide the guideline and foundation of how the company operates. Security policies will provide that mechanism to inform and remind employees that information security is an inherent part of this company's culture.

Employee owned companies may tend to operate their business on a less policy oriented methodology. Again, because they are owners of the company the attitude is often, "yes lets have policies, but these policies really don't apply to me, they're for the employees not the owners."

The assumption is that if the first four steps of this process have been successful, then the "culture" of the company is such that the adoption of security policies is embraced by all. A good security policy will identify acceptable or unacceptable behavior and explain what the consequence is if the policy is breached.

Communicating the policies is another challenge that is often under estimated especially if your organization is geographically spread out. It's not good enough to create good policies; they must be communicated to all employees and must be reviewed on a regular basis. Again finding a mechanism that works in your organization is key.

4. Conclusion/Summary

Information security is no longer an option it's a fundamental part of running a business today. Every company that uses computers and the internet must have a good sound security strategy and having a security aware culture is the beginning of a good sound security strategy. Five to ten years from now information security will be inherent in every organization and those organizations that have the culture to easily adapt to the changes required to protect the organizations' assets will have the advantage.

The senior managers (majority shareholders) in an employee owned company typically have never had to worry about information security throughout the majority of their careers so we need to educate them in this area. Developing an information security aware attitude in the company is the goal to developing an information security aware

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

culture. The employees/owners of the company need to understand their risks, their role and need to be involved in the process.

The concept of developing an information security aware company is not a matter of if it should happen; it's a matter of when it will happen. Any organization that uses the internet as a tool will have to adhere to good information security practices in order to stay in business.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal. Essentials with CISSP CBK Version 2.1 Volume One. April 2003.

Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal. Essentials with CISSP CBK Version 2.1 Volume Two. April 2003.

Chen, Anne "Mitnick to IT managers: 'Everybody is suspect'." 2 October 2000 http://www.zdnetindia.com/news/breaknews/stories/4633.html

Cobweb Applications Ltd. "What is information Security?" http://www.cobwebapplications.co.uk/is/

Crass, Stephen "Hackers Prove People are the Weakest Link." 1 August 2002 http://www.spectrum.ieee.org/WEBONLY/resource/aug02/hackers.html

Hurley, Edward. "Security's weakest link: People." 16 May 2002, Search Security. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci824195,00.html

Curtin, Matt. Developing Trust: Online Privacy and Security; Apress, Berkeley, CA, 2002

Skoudis, Ed. Counter Hack; Prentice Hall PTR, Upper Saddle River, NJ, 2002

Garfinkel, Simson with Spafford, Gene. Web Security & Commerce; O'Reilly & Associates Inc., 1997

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.